PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-162965
(43)Date of publication of application : 16.06.2000

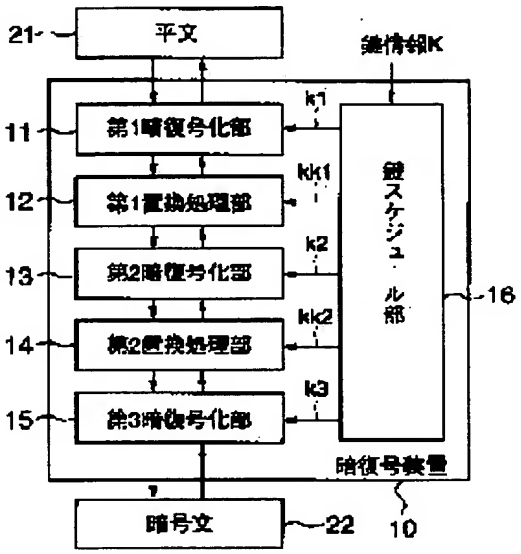
(51)Int.Cl. G09C 1/00

(21)Application number : 10-337108
(22)Date of filing : 27.11.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : SANO FUMIHIKO
KAWAMURA SHINICHI
SHIMIZU HIDEO

(54) CIPHERING AND DECIPHERING DEVICE, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an algorithm more efficient than a simple three-staged DES-SS and also resistant to a difference attack and a linear attack, although it configures a single encription algorithm compatible to any of DES, triple DES, and DES-SS.
SOLUTION: This device is a ciphering and deciphering device 10 which ciphers a plain text 21 into a cipher-text 22 and/or decipher a cipher-text into a plain text, and is provided with a 1st ciphering and deciphering means 11 for processing by ciphering or decipher processing, a 1st substituting means 12 for substituting a data for an output of the 1st ciphering and deciphering means according to a substitution table, a 2nd ciphering and deciphering means 13 for processing an output of the 1st substituting means by ciphering or deciphering, a 2nd substituting means 14 for substituting a data for the output of the 2nd ciphering and deciphering means according to a predetermined substitution table, and a 3rd ciphering and deciphering means 15 for ciphering or deciphering an output of the 2nd substituting means.



LEGAL STATUS

[Date of request for examination]	06.02.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3679936
[Date of registration]	20.05.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－162965
（P2000－162965A）
(43)公開日　平成12年６月16日(2000.6.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｂ	５Ｊ１０４

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－337108

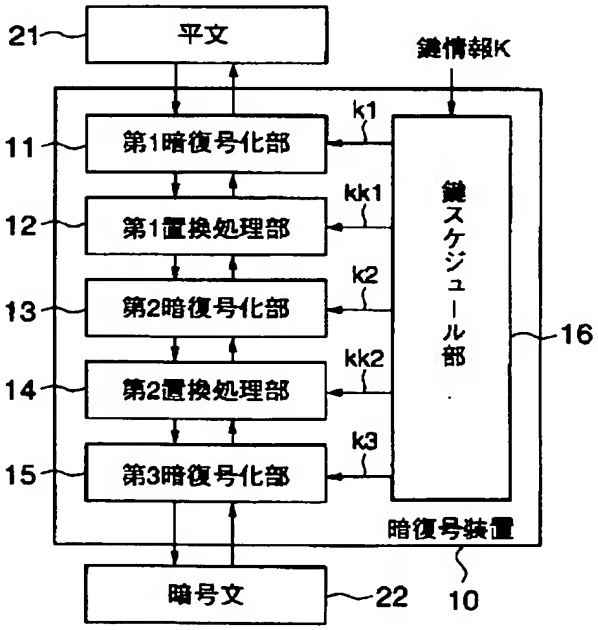
(22)出願日　平成10年11月27日(1998.11.27)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　佐野　文彦
東京都府中市東芝町１番地　株式会社東芝府中工場内
(72)発明者　川村　信一
東京都府中市東芝町１番地　株式会社東芝府中工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　暗復号装置及び記憶媒体

(57)【要約】
【課題】　本発明は、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳのすべてと互換な単一の暗号アルゴリズムを構成するが、単にＤＥＳ－ＳＳを３段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる。
【解決手段】　平文２１を暗号文２２に暗号化し、及び又は、暗号文を平文に復号する暗復号装置１０であって、暗号処理又は復号処理を行う第１の暗復号化手段１１と、第１の暗復号化手段の出力を所定の置換表によりデータ置換する第１の置換手段１２と、第１の置換手段の出力に対し、暗号処理又は復号処理を行う第２の暗復号化手段１３と、第２の暗復号化手段の出力を所定の置換表によりデータ置換する第２の置換手段１４と、第２の置換手段の出力に対し、暗号処理又は復号処理を行う第３の暗復号化手段１５とを備えた暗復号装置



1

【特許請求の範囲】

【請求項１】　平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置であって、
暗号処理又は復号処理を行う第１の暗復号化手段と、
前記第１の暗復号化手段の出力を所定の置換表によりデータ置換する第１の置換手段と、
前記第１の置換手段の出力に対し、暗号処理又は復号処理を行う第２の暗復号化手段と、
前記第２の暗復号化手段の出力を所定の置換表によりデータ置換する第２の置換手段と、
前記第２の置換手段の出力に対し、暗号処理又は復号処理を行う第３の暗復号化手段とを備えたことを特徴とする暗復号装置。

【請求項２】　前記第１の暗復号化手段と前記第３の暗復号化手段、並びに、前記第１の置換手段と前記第２の置換手段は、それぞれ同一のアルゴリズムに従う手段となることを特徴とする請求項１記載の暗復号装置。

【請求項３】　前記第１，第２及び第３の暗復号化手段並びに前記第１及び第２の置換手段それぞれに与える中間鍵を生成する鍵生成手段を備えるとともに、
前記第１及び第２の置換手段は、前記鍵生成手段が生成した中間鍵に所定の情報が含まれているときには恒等変換として機能することを特徴とする請求項１又は２記載の暗復号装置。

【請求項４】　前記第１及び又は第３の暗号復号化手段は、前記鍵生成手段が生成した中間鍵に所定の情報が含まれているときには、前記第２の暗号復号化手段と同一のアルゴリズムに従う手段となることを特徴とする請求項３記載の暗復号装置。

【請求項５】　前記第２の暗復号化手段は、前記第１及び第３の暗号復号化手段が暗号化処理を行うときには復号処理を実行し、前記第１及び第３の暗号復号化手段が復号処理を行うときには暗号化処理を実行することを特徴とする請求項３又は４記載の暗復号装置。

【請求項６】　前記鍵生成手段は、前記第１及び第３の暗号復号化手段に同一の中間鍵を与えることを特徴とする請求項５記載の暗復号装置。

【請求項７】　前記鍵生成手段は、前記第１及び第２の暗号復号化手段、又は、前記第２及び第３の暗号復号化手段が同一アルゴリズムとなりかつ同一暗復号鍵を使用する結果となる中間鍵を与えることを特徴とする請求項５記載の暗復号装置。

【請求項８】　平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置を制御するプログラムであって、
暗号処理又は復号処理を行わせる第１の暗復号化手段と、
前記第１の暗復号化手段の出力を所定の置換表によりデータ置換させる第１の置換手段と、
前記第１の置換手段の出力に対し、暗号処理又は復号処理を行わせる第２の暗復号化手段と、
前記第２の暗復号化手段の出力を所定の置換表によりデータ置換させる第２の置換手段と、
前記第２の置換手段の出力に対し、暗号処理又は復号処理を行わせる第３の暗復号化手段とを有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項９】　前記第１，第２及び第３の暗復号化手段並びに前記第１及び第２の置換手段それぞれに与える中間鍵を生成させる鍵生成手段を備えるとともに、
前記第１及び第２の置換手段を、前記鍵生成手段が生成させた中間鍵に所定の情報が含まれているときには恒等変換として機能させることを特徴とする請求項８記載の記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は暗復号装置及び記憶媒体、特に秘密鍵ブロック暗号により情報を暗号化若しくは復号するのに適した暗復号装置及び記憶媒体に関するものである。

【０００２】

【従来の技術】近年の計算機通信技術の発達に伴い、種々の情報がデジタル情報として通信され、また蓄積されるようになっているが、これらの情報についての機密やプライバシーを保護するために情報を暗号化する必要性が増している。このために、従来は主にＤＥＳ方式（特開昭５１－１０８７０１）を用いることで、情報の暗号を図っている。

【０００３】しかしながら、ＤＥＳ方式（以下、単にＤＥＳともいう）は１９７０年代に設計された暗号アルゴリズムであり現代の技術進歩に対して安全であるとは言えなくなってきている。ＤＥＳに対する解読攻撃方法としては、５６ビットからなる鍵の総当り探索や総当り探索より効率のよい差分攻撃（Ｅ．Ｂｉｈａｍ ａｎｄ Ａ．ｓｈａｍｉｒ，“Ｄｉｆｆｅｒｅｎｔｉａｌ Ｃｒｙｐｔａｎａｌｙｓｉｓ ｏｆ ＤＥＳ－ｌｉｋ Ｃｒｙｐｔｏｓｙｓｔｅｍｓ，”Ｊｏｕｒｎａｌ ｏｆ ＣＲＹＰＴＯＬＯＧＹ，Ｖｏｌ．４，Ｎｕｍｂｅｒ １，１９９１）、線形攻撃（松井充，ＤＥＳ暗号の線形解読法（Ｉ），暗号と情報セキュリティシンポジウム、１９９３）等が知られている。

【０００４】このような状況から既に広く普及しているＤＥＳ方式を大幅に変更することなく、解読攻撃に対する防御力を強化する試みとして、トリプルＤＥＳが知られている。

【０００５】トリプルＤＥＳは暗号化を行うのにＤＥＳを３回適用する方式であり、２つの鍵を使用して、鍵１による暗号化、鍵２による復号、鍵１による暗号化、という手順により暗号化を行うものである。トリプルＤＥＳではＤＥＳの鍵を２つ用いるので個々の鍵は５６ビットでありながら、実質的な鍵の長さは１１２ビットであ

ると考えることができる。

【０００６】しかし、トリプルＤＥＳはＤＥＳを３回行うため、ＤＥＳと較べて処理時間が多くかかってしまうという問題点がある。

【０００７】一方、ＤＥＳを強くしようとする異なる試みとして、ＤＥＳ－ＳＳ方式（特開平１０－１１６０２９）が知られている。

【０００８】ＤＥＳ－ＳＳ方式（以下、単にＤＥＳ－ＳＳともいう）では、ＤＥＳ内部で使用されている非線型関数であるＦ関数の他に新たにＧ関数を用いることで、ＤＥＳの安全性を高めている。また、ＤＥＳ－ＳＳの処理ではＤＥＳと比較するとＧ関数の処理が増加しているだけなので、トリプルＤＥＳと較べて効率がよいという特徴を持つ。

【０００９】さらに、トリプルＤＥＳとは異なり５６ビットの鍵を複数用いるのでなく、１個の鍵自体の長さが１１２ビットであるため、総当り攻撃に対してより安全であるという特徴も持っている。

【００１０】ＤＥＳの５６ビットの鍵は８ビットのパリティビットを含めて６４ビットで表される。ＤＥＳ－ＳＳでは、鍵の上位６４ビットと下位６４ビットが同じ値である場合には、ＤＥＳと同じ機能を果たす暗号化関数として動作するという他の暗号方式にない特徴がある。これによりＤＥＳ－ＳＳを有する暗復号装置では、ＤＥＳ互換モードを設けることが可能になる。

【００１１】このＤＥＳ互換モードの原理は、鍵の上位と下位が等しい場合には、Ｇ関数の入力と出力が一致する関数、すなわち恒等変換であることに基づいている。ＤＥＳ－ＳＳのもつＤＥＳ互換モードを利用することにより、１つの暗復号装置で２つの暗号化を行うことができ、装置規模を小さくできるという利点がある。

【００１２】

【発明が解決しようとする課題】上記したように、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳにはそれぞれ長所と短所がある。ここで、情報暗号化の要請及び高強度の必要性がますます高くなっていること、及び、ＤＥＳは広く普及していること、等の事情を考え合わせれば、ＤＥＳ及びその応用暗号化技術との互換性を確保しつつ強度の高い暗号化も可能な技術を提供することが重要になってきている。

【００１３】しかし、この技術の実現にあたっては、暗号の効率性という点も考慮に入れなければならない。

【００１４】例えばＤＥＳ－ＳＳを用いれば、ＤＥＳより安全でトリプルＤＥＳより効率のよい暗号化を行うことができる。ここでＤＥＳ－ＳＳを用いてトリプルＤＥＳと互換性のある暗号を構成しようとする場合を考える。ＤＥＳ－ＳＳを３段重ねることでトリプルＤＥＳと互換性のある暗号を実現することは可能ではあるが、トリプルＤＥＳ以上に効率が悪くなるという問題がある。

【００１５】一方、ＤＥＳ、トリプルＤＥＳ及びＤＥＳ－ＳＳの何れもラウンド関数を利用し、同じ構造の処理を繰り返し行う積暗号と呼ばれる形式を用いている。このような形式の暗号は、上記した差分攻撃や線形攻撃に弱いという特徴を持っている。

【００１６】本発明は、このような実情を考慮してなされたもので、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳのすべてと互換な単一の暗号アルゴリズムを構成するが、単にＤＥＳ－ＳＳを３段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる暗復号装置及び記憶媒体を提供することを目的とする。

【００１７】

【課題を解決するための手段】上記課題を解決するために、請求項１に対応する発明は、平文を暗号文に暗号化し、及び又は、暗号文を平文に復号する暗復号装置であって、暗号処理又は復号処理を行う第１の暗復号化手段と、第１の暗復号化手段の出力を所定の置換表によりデータ置換する第１の置換手段と、第１の置換手段の出力に対し、暗号処理又は復号処理を行う第２の暗復号化手段と、第２の暗復号化手段の出力を所定の置換表によりデータ置換する第２の置換手段と、第２の置換手段の出力に対し、暗号処理又は復号処理を行う第３の暗復号化手段とを備えた暗復号装置である。

【００１８】本発明はこのような手段を設けたので、各暗復号化手段の内容及び各置換手段の使用有無を調整することで、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳのすべてと互換な単一の暗号アルゴリズムを構成するが、単にＤＥＳ－ＳＳを３段重ねるより効率がよいものとすることができる。また、置換手段によりデータ置換を行えば、データの連続性に擾乱が与えられるので、差分攻撃や線形攻撃にも強いアルゴリズムとすることができる。

【００１９】次に、請求項２に対応する発明は、請求項１に対応する発明において、第１の暗復号化手段と第３の暗復号化手段、並びに、第１の置換手段と第２の置換手段は、それぞれ同一のアルゴリズムに従う手段となる暗復号装置である。

【００２０】本発明はこのような手段を設けたので、より簡単な構成で請求項１に係る発明と同様な効果を得ることができる。

【００２１】次に、請求項３に対応する発明は、請求項１又は２に対応する発明において、第１，第２及び第３の暗復号化手段並びに第１及び第２の置換手段それぞれに与える中間鍵を生成する鍵生成手段を備えるとともに、第１及び第２の置換手段は、鍵生成手段が生成した中間鍵に所定の情報が含まれているときには恒等変換として機能する暗復号装置である。

【００２２】本発明はこのような手段を設けたので、第１及び第２の置換手段に与える中間鍵の内容を制御することで、ＤＥＳ、トリプルＤＥＳ等の互換モードとそれ以外の強化暗号モードを容易に切り換えることができる。

【００２３】次に、請求項４に対応する発明は、請求項３に対応する発明において、第１及び又は第３の暗号復号化手段は、鍵生成手段が生成した中間鍵に所定の情報が含まれているときには、第２の暗号復号化手段と同一のアルゴリズムに従う手段となる暗復号装置である。

【００２４】本発明はこのような手段を設けたので、第１～第３の暗復号化手段に与える中間鍵の内容を制御することで、ＤＥＳ、トリプルＤＥＳ等の互換モードにおける各モード切替を容易に行うことができる。

【００２５】次に、請求項５に対応する発明は、請求項３又は４に対応する発明において、第２の暗復号化手段は、第１及び第３の暗号復号化手段が暗号化処理を行うときには復号処理を実行し、第１及び第３の暗号復号化手段が復号処理を行うときには暗号化処理を実行する暗復号装置である。

【００２６】本発明はこのような手段を設けたので、容易にトリプルＤＥＳやＤＥＳ、ＤＥＳ－ＳＳ間の切り替えを行うことができる。

【００２７】次に、請求項６に対応する発明は、請求項５に対応する発明において、鍵生成手段は、第１及び第３の暗号復号化手段に同一の中間鍵を与える暗復号装置である。

【００２８】本発明はこのような手段を設けたので、容易にトリプルＤＥＳを実現することができる。

【００２９】次に、請求項７に対応する発明は、請求項５に対応する発明において、鍵生成手段は、第１及び第２の暗号復号化手段、又は、第２及び第３の暗号復号化手段が同一アルゴリズムとなりかつ同一暗復号鍵を使用する結果となる中間鍵を与える暗復号装置である。

【００３０】本発明はこのような手段を設けたので、容易にＤＥＳやＤＥＳ－ＳＳを実現することができる。

【００３１】次に、請求項８に対応する発明は、請求項１に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００３２】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項１の暗復号装置として機能する。

【００３３】次に、請求項９に対応する発明は、請求項６に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００３４】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項３の暗復号装置として機能する。

【００３５】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第１の実施の形態）図１は本発明の第１の実施形態に係る暗復号装置の一例を示す構成図である。

【００３６】この暗復号装置１０は、第１，第２，第３暗復号化部１１，１３，１５、第１，第２置換処理部１２，１４並びに鍵スケジュール部１６を備える他、各機能部１１～１６を制御する制御部（図示せず）を備えて、暗号化装置、復号装置あるいは暗号化・復号装置として構成される。

【００３７】ここで、平文２１を第１暗復号化部１１に入力し、第１置換処理部１２、第２暗復号化部１３、第２置換処理部１４、第３暗復号化部１５と処理を進めて暗号文２２を出力する場合には暗号装置として機能し、暗号文２２を第３暗復号化部１５に入力し、上記と逆方向に処理を進める場合には復号装置として機能する。この何れの装置として、機能させるかは制御部の処理によって決まることになる。

【００３８】また、暗復号装置１０は、ハードウエア的にはＣＰＵやメモリ等の計算機要素から構成されるものである。各機能部１１～１６はこの計算機要素が所定のプログラムに制御されて実現される。すなわち機能部１１～１６はハードウエア資源とソフトウエア資源の結合たる機能実現手段である。また、上記計算機要素及びプログラムは、パーソナルコンピュータやワークステーション等の計算機に提供されるものを使用するか、専用のチップを作成することにより、本暗復号装置１０用に確保される。

【００３９】次に、上記各機能部１１～１６の構成について説明する。

【００４０】まず、鍵スケジュール部１６は、外部から入力された鍵情報Ｋをもとに中間鍵に展開し、機能部１１～１５からなるデータ撹拌部に供給する。

【００４１】機能部１１～１５からなるデータ撹拌部は、６４ビット入力の平文２１又は暗号文２２を、鍵スケジュール部１６からの鍵により撹拌して暗号化しあるいは復号し、対応する暗号文２２若しくは平文２１として出力する。

【００４２】ここで、第１暗復号部１１は、ＤＥＳ－ＳＳのデータ撹拌部と同様な構成を備え、平文２１を入力され、鍵スケジュール部１６から入力された中間鍵の制御下で暗号化処理としての撹拌処理を行い、出力を第１置換処理部１２に入力する。逆に、第１置換処理部１２からの入力を鍵スケジュール部１６からの中間鍵で復号し、平文２１として出力する。なお、復号処理については、ここで説明したように暗号化処理の逆の処理を行うだけなので、以下の機能部１２～１５の説明においては暗号化を行う場合についてのみ説明し、特に断らない限り復号については省略する。

【００４３】また、この第１暗復号部１１は、ＤＥＳ－ＳＳの構成を有することから、鍵スケジュール部１６からの中間鍵の内容が一定の場合には単なるＤＥＳとして機能する。なお、ＤＥＳ－ＳＳについては第２の実施形態で詳しく説明する。

【００４４】第１置換処理部１２は、第１暗復号処理部１１から入力されたデータについて、中間鍵及び置換表

を用いたデータの置換処理を行い、その出力を第２暗復号化部１３に入力する。また、中間鍵が一定の場合にはこの第１置換処理部１２を未使用状態にできるようになっている。未使用状態の場合は入力データをそのまま出力する。ここで、置換表は、乱数によって生成する方法若しくは代数的に生成する方法（式を用いる方法）によって作成される。何れの場合も差分確率及び線形確率の低い、すなわち差分攻撃や線形攻撃に強い置換表を作成する。

【００４５】図２は置換処理部等に用いられる差分確率及び線形確率の低い置換表の一例を示す図である。

【００４６】このような表は、差分確率及び線形確率の良好（低く）にできる代数式（例えば有限体ＧＦ（２＾８）上で原始多項式（ｘ＾８＋ｘ＾４＋ｘ＾３＋ｘ＾２＋１）を用いてｘ＾（－１）を計算する；“＾”は冪乗演算）を用いるか、差分確率及び線形確率が良くなるまで乱数計算を繰り返して作成する。

【００４７】なお、本実施形態において差分確率及び線形確率が良好であるためには、それぞれの確率が理想値の２倍以下であることが望ましい。ここで８ビットの場合であれば、差分確率の理想値は４／２５６であり、線形確率の理想値は１６／２５６である。

【００４８】次に第２暗復号化部１３は、ＤＥＳのデータ攪拌部と同様な構成を備え、第１置換処理部１２からの出力に対し、鍵スケジュール部１６からの中間鍵の制御下で攪拌処理を行い、その出力を第２置換処理部１４に入力する。なお、ここにおける攪拌処理は暗号文２２を生成するための復号処理である。逆に平文２１に復号するためには暗号処理がなされる。

【００４９】第２置換処理部１４は、第１置換処理部１３と同様な構成を備え、中間鍵および置換表を用いたデータの置換処理を行い、出力を第３暗復号化部１５に入力する。また、中間鍵が一定の場合には第２置換処理部１４を未使用状態、すなわち入力と出力が一致するようになっている。

【００５０】第３暗復号部１５は、ＤＥＳ－ＳＳのデータ攪拌部と同様な構成を備え、鍵スケジュール部１６から入力された中間鍵の制御下で暗号化処理としての攪拌処理を行い、暗号文２２を出力する。また、第３暗復号部１５もＤＥＳ－ＳＳの構成を有するので、鍵スケジュール部１６からの中間鍵の内容が一定の場合には単なるＤＥＳとして機能する。

【００５１】次に、以上のように構成された本実施形態における暗復号装置の動作について説明する。

【００５２】この暗復号装置においては、鍵スケジュール部１６からの中間鍵により、第１，第３暗復号処理部１１，１５を、”ＤＥＳ”、”ＤＥＳ－ＳＳ”の何れか、また第１，第２置換処理部１２，１４を、”使用”、”未使用”の何れかの状態に選択できるようになっている。これにより各機能部１１～１５の状態組み合わせを適宜に変更可能である。

【００５３】図３は各機能部の状態組み合わせの例を示す図である。

【００５４】同図において、まず、第１，第３暗復号化部１１，１５をＤＥＳモードにし、第１，第２置換処理部１２，１４を未使用の状態にするとともに、第１，第２暗復号化部１１，１３に使用する鍵を同一にすると、暗復号装置全体はＤＥＳによる暗復号装置となる。

【００５５】これは、第２暗復号化部１３が平文２１の暗号化に際して復号処理を行うため、第１暗復号処理部１１で暗号化されたデータが第２暗復号化部１３によって元の平文２１に戻ってしまうためである。

【００５６】次に、第１，第２，第３暗復号化部１１，１３，１５をＤＥＳモードにし、第１，第２置換処理部１２，１４を未使用状態とすると、トリプルＤＥＳと同一の状態になる。トリプルＤＥＳは、平文を第１の鍵で暗号化し、その出力を第２の鍵で復号し、さらにその出力を第１の鍵で暗合する方式である。ここでは、第１暗復号化部１１が上記最初の暗号化を担当し、第２暗復号化部１３が次の復号を担当し、第３暗復号化部１５が最後の暗号化を担当する。

【００５７】次に、第１暗復号化部１１をＤＥＳモードにし、第１，第２置換処理部１２，１４を未使用状態とするとともに、第１，第２暗復号化部１１，１３に同一の鍵を使用するとＤＥＳ－ＳＳモードと同一の状態になる。上記の場合と同様に、第１，第２暗復号化部１１，１３の処理は互いにうち消し合って、平文２１が第３暗復号化部１５に入力される状態になるためである。

【００５８】以上が本実施形態の暗復号装置１０の有するＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳ互換モードである。

【００５９】次に、第１，第２置換処理部１２，１４を使用する場合には、上記互換モードよりも強化された暗号化を行うモードとなる。以下に説明する各場合は、第１，第２置換処理部１２，１４を使用するものである。

【００６０】例えば第１，第２，第３暗号化部１１，１３，１５すべてをオリジナルのモード（ＤＥＳ－ＳＳ、ＤＥＳ、ＤＥＳ－ＳＳ）で使用した場合（図３：パターン１）、トリプルＤＥＳとＤＥＳ－ＳＳを組み合わせ、さらに各処理間に置換表による攪拌を加えたものとなる。

【００６１】この場合、ＤＥＳ方式に類するラウンド関数の繰り返しによるデータ攪拌がＤＥＳ－ＳＳの長い鍵で十分に行われるとともに、各処理間で差分確率及び線形確率の低い置換表による攪拌が加えられるので、データの連続性に擾乱がおこり、線形攻撃や差分攻撃といった攻撃に対する防御力が強くなる。

【００６２】また、第１，第３暗復号化部１１，１５をＤＥＳとし（図３：パターン２）、線形攻撃等からの防御力を保持しつつ、パターン１に比べて暗号化時間の短

縮化を図るようにすることも可能である。

【００６３】さらに、第１，第３暗復号化部１１，１５の一方をＤＥＳとし、他方をＤＥＳ－ＳＳとしてパターン１とパターン２の中間的な暗号とすることも可能である。

【００６４】また、上記各パターンの場合に、各暗復号化部１１，１３，１５に与える鍵の組み合わせを変更して更に種々の暗号形式とすることができる。例えば暗復号化部１１，１３，１５すべてに異なる鍵を与える、暗復号化部１１，１３に同一の鍵を与える、暗復号化部１１，１５に同一の鍵を与える、暗復号化部１３，１５に同一の鍵を与える、暗復号化部１１，１３，１５すべてに同一の鍵を与える、等のパターンが考えられる。

【００６５】これらは、暗復号化装置１０の処理能力や、互換モード及び強化暗号モードにおける各パターンの普及度等を考慮して適宜選択される。

【００６６】上述したように、本発明の実施の形態に係る暗復号装置は、第１，第２，第３暗復号化部１１，１３，１５を設け、各処理部の動作モード及び与える鍵を適宜変更できるようにしたので、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳのすべてと互換な単一の暗号アルゴリズムを構成するが、ＤＥＳ－ＳＳを３段重ねるより効率のよい暗号アルゴリズムの装置として構成することができる。したがって、このような暗号アルゴリズムの装置では独立して３つの暗号装置を持つよりも、装置規模を小さくすることができる。

【００６７】また、本実施形態の暗復号装置１０は、置換処理部１２，１４によって、データの連続性に擾乱を起こすことができるので、線形攻撃や差分攻撃等の同一構成の繰返しに着目した攻撃をより困難にすることができ、安全性を向上させることができる。

【００６８】また、本実施形態の装置では、単一のアルゴリズムで種々の暗号方式を提供できるので、各暗号の普及度やハードウエアの処理能力の変化に応じて使用する暗号方式を選択することができ、長期間に渡って使用することができる。

（発明の第２の実施の形態）本実施形態では、第１の実施形態における各機能部１１～１６の構成をより具体化させた場合について説明する。したがって、本実施形態は第１の実施形態と同様に構成される他、各機能部１１～１６における更なる形態例が示されるものである。

【００６９】本実施形態の暗復号装置１０は、図１に示す第１の実施形態の暗復号装置と同様に構成されている。以下、各機能部１１～１６の構成例を説明する。なお、本実施形態の各図面においては、第１実施形態の図１と同一部分には同一符号を付して詳細説明を省略する。

［鍵スケジュール部１６の構成動作］まず、鍵スケジュール部１６について説明する。

【００７０】図４は鍵スケジュール部の全体構成を示す図である。

【００７１】同図に示すように、鍵スケジュール部１６には、２５６ビットの鍵情報Ｋを５つに分割し各レジスタ３２，３３，３４，３５，３６に格納する分割部３１と、レジスタ３２～３５から５６ビットの鍵情報を読出しこれを拡大転置して６４ビットにする拡大転置部３７とが設けられている。さらに、拡大転置結果若しくはレジスタ３６の内容から中間鍵Ｋ１，Ｋ２，Ｋ３並びにＫＫ１及びＫＫ２をそれぞれ生成するＤＥＳ－ＳＳ鍵スケジュール部３８，３９、ＤＥＳ鍵スケジュール部４０及び置換用鍵スケジュール部４１が設けられ、鍵スケジュール部１６が構成されている。

【００７２】ここで２５６ビットの鍵情報は、分割部３１において５６ビットからなる４つのブロックＢ１，Ｂ２，Ｂ３，Ｂ４と、３２ビットの１つのブロックＢ５に分割され、それぞれレジスタ３２～３６に記憶される。この場合の分割の仕方は、２５６ビットを先頭から順次５６ビットづつ切り出してそれぞれＢ１～Ｂ４とし、さらに最後の残り３２ビットをＢ５とするものである。

【００７３】また、ブロックＢ１からブロックＢ４までの４つのブロックはそれぞれ拡大転置部３７に入力され、それぞれ拡大転置表によって６４ビットに拡大される。

【００７４】図５は拡大転置表の一例を示す図である。

【００７５】同図の表は先頭から出力ビットに対応しており、また各出力ビットにおける数字は入力が第ｎビット目であるかをあらわす。ただし、表中の０はその出力ビットとして０が出力されることを表す。

【００７６】次に、ブロックＢ１を拡大した６４ビットの鍵とブロックＢ２を拡大した６４ビットの鍵を連結した１２８ビットの鍵は、第１暗復号部１１への中間鍵Ｋ１を出力するＤＥＳ－ＳＳ鍵スケジュール部３８に入力される。

【００７７】また、ブロックＢ１を拡大した６４ビットの鍵とブロックＢ３を拡大した６４ビットの鍵を連結した１２８ビットの鍵は、第３暗復号部１５への中間鍵Ｋ３を出力するＤＥＳ－ＳＳ鍵スケジュール部３９に入力される。

【００７８】また、ブロックＢ４を拡大した６４ビットの鍵は、第２暗復号部１５への中間鍵Ｋ２を出力するＤＥＳ鍵スケジュール部４０に入力される。さらに、３２ビットのブロックＢ５は拡大転置されることなく置換用鍵スケジュール部４１に入力される。

【００７９】上記各鍵スケジュール部３８～４１のうち、ＤＥＳ鍵スケジュール部４０は一般的なＤＥＳにおける拡大鍵生成手段と同様な構成を有するのみであるので、詳細説明は省略し、以下、ＤＥＳ－ＳＳ鍵スケジュール部３８，３９及び置換用鍵スケジュール部４１について説明する。

【００８０】図６はＤＥＳ－ＳＳ鍵スケジュール部の構

成例を示すブロック図である。

【００８１】ＤＥＳ－ＳＳ鍵スケジュール部３８，３９は、Ａスケジュール部４５，Ｂスケジュール部４６及びＦＧ拡大鍵生成部４７から構成される。なお、ＦＧ拡大鍵生成部４７は各ラウンド（１段～１６段）に対応して設けられるとともに、Ａスケジュール部４５及びＢスケジュール部４６内も１６段の構成となっており、同図にはそれぞれ第１段のみが示されている。なお、符号以外の同図における数値はビット数を現している。

【００８２】拡大転置部３７から入力される１２８ビットの鍵のうち、各ブロックＢ１，Ｂ２若しくはＢ３に対応する部分がそれぞれＡスケジュール部４５，Ｂスケジュール部４６に入力されるようになっている。

【００８３】Ａスケジュール部４５及びＢスケジュール部４６は、入力される鍵が異なり、また拡大鍵を生成するためのデータの出力の仕方が異なる点を除けば、一般的なＤＥＳにおける拡大鍵生成手段と同様な構成となっているので詳細説明は省略する。

【００８４】ここで、ＤＥＳ－ＳＳ用とＤＥＳ用の中間鍵における相違点は、ＤＥＳ－ＳＳではＤＥＳの攪拌手段に使用されるＦ関数拡大鍵に加え、Ｇ関数拡大鍵が必要な点である。

【００８５】図６におけるＡスケジュール部４５及びＢスケジュール部４６では、ビット選択部４８Ａ，４８Ｂが中間鍵Ｋ１／Ｋ２を生成するための情報を出力する。

【００８６】ここでまず、Ａスケジュール部４５のビット選択部４８Ａは、Ｆ関数拡大鍵ＦＫ１を出力するとともに、５ビットの鍵Ａ１を出力する。この５ビットの鍵Ａ１は例えばビット選択部４８Ａに入力されてなる５６ビットの鍵の左から９，１８，２２，２５，３５番目の５ビットが用いられる。この５ビット選択方法は他の方法でも良い。

【００８７】一方、Ｂスケジュール部４のビット選択部４８Ｂは、Ｇ関数拡大鍵の元になる４８ビットの鍵ＧＢ１を出力するとともに、鍵Ａ１と同様な５ビットの鍵Ｂ１を出力する。Ａスケジュール部４５及びＢスケジュール部４６が一般的なＤＥＳの拡大鍵生成手段と異なるのは、ビット選択部４８Ａ，４８Ｂ（以下の、２～１６段も同様）の処理がこのように修正されている点のみである。

【００８８】ＦＧ拡大鍵生成部４７は、ビット選択部４８Ａが出力した鍵をそのままＦ関数拡大鍵ＦＫ１として出力する。また、４８ビットの鍵ＧＢ１とＦ関数拡大鍵ＦＫ１の排他的論理和４９をとってＧ関数拡大鍵ＧＫ１の一部（Ｇ１，Ｇ２，Ｇ３）として出力する。さらにＦＧ拡大鍵生成部４７は、鍵Ａ１と鍵Ｂ１との間で排他的論理和５０を取り、さらにその出力と０Ｘ１０（０Ｘは１６進を表す）との間で排他的論理和５１をとってＧ関数拡大鍵ＧＫ１の一部（Ｇ４）として出力する。

【００８９】こうして、ＤＥＳ－ＳＳ鍵スケジュール部３８，３９によって、Ｆ関数拡大鍵ＦＫ１と、鍵Ｇ１，Ｇ２，Ｇ３，Ｇ４からなるＧ関数拡大鍵ＧＫ１とを含む中間鍵Ｋ１，Ｋ３が得られる。

【００９０】ＤＥＳ－ＳＳ鍵スケジュール部３８が出力した中間鍵Ｋ１は第１暗復号化部１１に入力され、ＤＥＳ－ＳＳ鍵スケジュール部３９が出力した中間鍵Ｋ３は第３暗復号化部１５に入力されることとなる。なお、詳細説明は省略したが、ＤＥＳ鍵スケジュール部４０が出力した中間鍵Ｋ２は第２暗復号化部１３に入力され、第２暗復号化部１３によって、ＤＥＳによる暗復号が実行される。

【００９１】次に、置換用鍵スケジュール部４１について説明する。

【００９２】図７は置換用鍵スケジュール部の構成例を示すブロック図である。

【００９３】この置換用鍵スケジュール部４１は、レジスタ３６のブロックＢ５を３２ビットの鍵として入力し、第１置換処理部１２に入力される中間鍵ＫＫ１と、第２置換処理部１４に入力される中間鍵ＫＫ２を出力するものである。

【００９４】まず、レジスタ５４内の３２ビットの鍵Ｃ０′は、そのまま第１置換処理部１２用の中間鍵ＫＤ１（３２ビット）として出力されるとともに、論理和部５５及び左シフト部５６に入力される。なお、レジスタ５４はレジスタ３６と同一であってもよい。

【００９５】論理和部５５では、３２ビットの鍵Ｃ０′における各ビットの論理和が計算結果として出力され、第１置換処理部１２用の中間鍵ＫＳ１（１ビット）となる。

【００９６】この中間鍵ＫＤ１と中間鍵ＫＳ１とから中間鍵ＫＫ１が構成され、第１置換処理部１２に入力される。

【００９７】次に、左シフト部５６に入力されたデータは同シフト部５６により４ビットほど左シフトされた後、鍵Ｃ１としてレジスタ５７に格納される。

【００９８】この鍵Ｃ１′は、第２置換処理部１４に入力される３２ビットの中間鍵ＫＤ２となり、また、論理和部５８において３２ビットＣ１′の論理和の計算結果が、第２置換処理部１４に入力される１ビットの中間鍵ＫＳ２となる。

【００９９】この中間鍵ＫＤ２と中間鍵ＫＳ２とから中間鍵ＫＫ２が構成され、第２置換処理部１４に入力される。

【０１００】以上が鍵スケジュール部１６の構成及び動作であり、次に、置換処理部１２，１４について説明する。

［置換処理部１２，１４の構成動作］図８は置換処理部の構成例を示すブロック図である。

【０１０１】同図に示すように置換処理部１２，１４は、初期転置部６１と、排他的論理和６２～６６と、置

換部６７～７４と、逆転置部７５とから構成されている。置換部６７～７４には、図２に示すような置換表が保持されており、入力を置換表により変換して出力する。

【０１０２】ここで、まず、暗復号化部からの６４ビットの入力は、初期転置（初期転置ＩＰ）部６１においてビット転置が行われ、その結果が８ビットづつの８つのブロックに分割される。

【０１０３】初期転置６１の出力のうち８ビットブロック４つからなる３２ビットはそのまま置換部６７～７０に入力される。残りの８ビットブロック４つからなる３２ビットは排他的論理和６２～６６において中間鍵ＫＤ（中間鍵ＫＤ１／ＫＤ２）との排他的論理和が行われ、その結果が置換部７１～７４に入力される。

【０１０４】置換部６７～７４には、８ビットの入力データと１ビットの鍵ＫＳ（中間鍵ＫＳ１／ＫＳ２）とが入力される。ここで、鍵ビットが１の場合には、置換表を用いた入力に対応する出力データが出力され、鍵ビットが０の場合には、入力と同一の出力データが出力される。すなわち鍵ＫＳが０ビットの場合には置換処理部１２，１４は未使用状態となる。

【０１０５】各置換部６７～７４からの出力は逆転置（逆転置IP^{-1}）７５に入力され、ここでビット転置が行われたのち、６４ビットデータとして出力される。

［第１，第３暗復号化部１１，１５の構成動作］次に、ＤＥＳ－ＳＳのデータ撹拌手段として構成される第１，第３暗復号化部１１，１５について説明する。

【０１０６】図９はＤＥＳ－ＳＳとして構成された暗復号化部の構成例を示すブロック図である。

【０１０７】ＤＥＳ－ＳＳとして構成された第１，第３暗復号化部１１，１５は、鍵ＧＫ及びＦＫからなる中間鍵Ｋ１又はＫ３に依存して入力（６４ビット）を撹拌し、対応する暗号文を出力する。この暗復号化部１１，１５は、初期転置部（初期転置ＩＰ）８０と、第１段から第１６段までのデータ撹拌部８１～９６と、最終転置部（最終転置IP^{-1}）９７とから構成されている。各データ撹拌部８１～９６は、暗号化関数としてのＦ関数８１ｆ～９６ｆ及び排他的論理和８１ａ～９６ａを備えてＤＥＳのデータ撹拌手段と同様に構成される他、鍵ＧＫを用いてデータを撹拌する暗号化関数としてのＧ関数８１ｇ～９６ｇをも備えている。

【０１０８】ここで、Ｆ関数８１ｆ～９６ｆは、通常のＤＥＳと同様な撹拌処理を行うものであり、中間鍵Ｋ１，Ｋ３のうちのＦ関数拡大鍵ＦＫとＧ関数８１ｇ～９６ｇの出力とを受け、所定の撹拌処理を行ってその結果を排他的論理和８１ａ～９６ａに入力する。

【０１０９】排他的論理和８１ａ～９６ａは、３２ビットのＬｎ（Ｌ０～Ｌ１５）とＦ関数８１ｆ～９６ｆの出力との間の排他的論理和を次段の入力の右側３２ビットＲｎ＋１として出力する。

【０１１０】また、Ｇ関数８１ｇ～９６ｇは、後述する撹拌処理を行うものであり、中間鍵Ｋ１，Ｋ３のうちのＧ関数拡大鍵ＧＫとＲｎ（Ｒ０～Ｒ１５）とを受け、所定の撹拌処理を行って次段の入力の左側３２ビットＬｎ＋１及びＦ関数８１ｆ～９６ｆへ出力する。

【０１１１】各段のデータ撹拌部８１～９６では同様な処理が実行される。まず第１段の動作について説明する。

【０１１２】暗復号化部１１，１５において、入力（６４ビット）は初期転置部８０にて転置された後、２つに等分割されて左側３２ビットＬ０と右側３２ビットＲ０として生成される。

【０１１３】第１段データ撹拌部８１において、Ｒ０は暗号化Ｇ関数８１ｇに入力され、そのＧ関数出力が暗号化Ｆ関数８１ｆに入力されるとともに、第２段データ撹拌部８２に左側３２ビットＬ１として出力される。一方、Ｌ０は排他的論理和部８１ａに入力され、Ｆ関数８１ｆとの間で排他的論理和が取られた後、第２段データ撹拌部８２に右側３２ビットＲ１として出力される。

【０１１４】以上の撹拌処理が第１段で行われたのち、以下、第１６段まで第１段と同様の撹拌処理が行われる。第１６段の出力は最終転置部９７によって転置が行われた後、６４ビットの出力となる。

【０１１５】次にＧ関数８１ｇ～９６ｇにおける処理について説明する。

【０１１６】図１０はＧ関数の構成例を示すブロック図である。

【０１１７】このＧ関数８１ｇ～９６ｇは、入力データに対し、Ｇ関数拡大鍵ＧＫに含まれる４つの鍵Ｇ１，Ｇ２，Ｇ３，Ｇ４を用いた撹拌を行ってデータ出力するものである。このために、Ｇ関数８１ｇ～９６ｇは、排他的論理和部１０３，１０４，１０８、論理積部１０１，１０６、左シフト部１０５を備えている。

【０１１８】なお、同図に示すＬ０′，Ｌ１′，Ｌ２′，Ｌ３′，Ｒ０′，Ｒ１′，Ｌ２′，Ｒ３′は、これらのデータがレジスタに格納され、あるいは次の機能手段に引き渡されることを示す。

【０１１９】このＧ関数においては、まず入力（３２ビット）は、２つに等分割されて左側３２ビットＬ０′と右側３２ビットＲ０′が生成される。

【０１２０】Ｒ０′は論理積部１０１及び排他的論理和部１０４に入力され、Ｌ０′は排他的論理和部１０３に入力される。

【０１２１】論理積部１０１においてＲ０′と拡大鍵Ｇ１の論理積が行われ、排他的論理和部１０３に出力される。排他的論理和１０３においてはＬ０′と論理積部１０１の出力との排他的論理和が行われ、その結果Ｌ１′が左シフト１０５に入力される。

【０１２２】一方、排他的論理和１０４においてはＲ０′と拡大鍵Ｇ２との排他的論理和が行われ、その結果

Ｒ１′が左シフト部１０５に入力される。

【０１２３】左シフト部１０５においては、拡大鍵Ｇ４のビット数に従った左シフトが行われ、そのシフト結果の出力は２つに等分割して左側３２ビットがＲ２′に、右側３２ビットがＬ２′となる。

【０１２４】Ｒ２′は論理積部１０６に入力され、Ｌ２′は排他的論理和部１０８に入力される。論理積部１０６においてはＲ２′と拡大鍵Ｇ３の論理積が行われ、排他的論理和部１０８に出力される。

【０１２５】さらに、排他的論理和部１０８において、Ｌ２′と論理積部１０６の出力との排他的論理和が行われ、Ｇ関数の出力の左側３２ビットとなる。一方、Ｇ関数の出力の右側３２ビットはＲ２′が用いられる。

【０１２６】このＧ関数においては、入力を分割しその分割入力を再び接続してシフトしつつ、その間に攪拌処理を挿入して出力データの攪拌度合いを高いものにしている。

［第２暗復号化部１３の構成動作］第２暗号化部１３は、一般的なＤＥＳのデータ攪拌手段と同様に構成されているので、ここでは詳細な説明は省略する。なお、ＤＥＳのデータ攪拌手段については（岡本栄司著，「暗号理論入門」，共立出版，１９９３）等に記載されている。また、例えば図９に示すＤＥＳ－ＳＳの構成からＧ関数８１ｇ～９６ｇを取り除きＧ関数拡大鍵ＧＫを不要としたものは、ＤＥＳのデータ攪拌手段の一例となっている。

［鍵情報Ｋに対応した暗復号装置１０の動作］本実施形態の暗復号装置１０の各機能部１１～１６が上記したように構成され動作するときに、鍵スケジュール部１６に与える鍵情報Ｋの内容により、暗復号装置１０がいかなる内容の暗号若しくは復号装置となるかについて説明する。

【０１２７】ここで、鍵情報Ｋは、図４に示すように、ブロックＢ１～Ｂ５に分割されるものであり、各ブロックＢ１～Ｂ５の内容がどのようになっているかにより本装置１０における処理が決まることになる。

【０１２８】まず、ブロックＢ５の部分に少なくともビットが立っており、その論理和５５，５８が０にならない場合には、鍵ＫＳが０とならずひいては図８に示す置換処理部１２，１４における置換部６７～７４において置換処理が実行される。この場合には、暗復号装置１０は、図３における強化暗号モードとして動作する。この結果、従来のＤＥＳ、ＤＥＳ－ＳＳ又はトリプルＤＥＳとは異なり、置換表による暗号連続性が擾乱された暗号となって、より強化された暗号化が実現される。

【０１２９】特に、ブロックＢ１からブロックＢ５の鍵情報として独立したものを与えれば、より安全性の高い２５６ビット鍵の暗号化アルゴリズムとして使用される。

【０１３０】一方、置換用鍵スケジュール部４１に入力される３２ビットの鍵ブロックＢ５の入力ビットがすべて０である場合には論理和５５，５８の出力である鍵ＫＳが０になるため、置換処理部１２及び１４における置換表が使用されない。したがって、この場合の中間鍵ＫＫ１，ＫＫ２によっては、置換処理部１２及び１４において、入力と同一のデータが出力され恒等変換が行われることになる。

【０１３１】置換処理部１２及び１４にて恒等変換が行われる場合には、暗復号装置１０は図３における互換モードとして動作することになる。以下、この場合について、更に具体的に説明する。

【０１３２】まず、図４において、ブロックＢ１と同一の内容をブロックＢ２及びＢ３に入力することにより、ＤＥＳ－ＳＳ鍵スケジュール部３８及び３９は、第１，第３暗復号化部１１，１５がＤＥＳ暗号化モードとなる暗号化処理を行う中間鍵を生成する。第１，第３暗復号化部１１，１５がＤＥＳモードになるためには、図９におけるＧ関数入出力が恒等変換となればよい。この恒等変換は、図１０に示すＧ関数処理において、拡大鍵Ｇ１～Ｇ４が所定の入力になれば実現される。

【０１３３】このとき、暗号化装置全体としては、ブロックＢ１に入力された鍵ビットによる第１暗復号化部１１のＤＥＳ暗号化と、ブロックＢ４に入力された鍵ビットによる第２暗復号化部１３のＤＥＳ復号の処理となり、５６ビットからなる２つの鍵を用いたトリプルＤＥＳと同一の処理内容となる。

【０１３４】この場合に、さらにブロックＢ１とブロックＢ４に同一の内容を用い、ブロックＢ２とＢ３のいずれか一方をブロックＢ１と同一の内容に設定することにより、ＤＥＳ－ＳＳとの互換モードとして動作する。これは、ブロックＢ１と同一内容を入力する側の暗復号化部１１又は１５がＤＥＳモードで動作して、第２暗復号化部１３の処理とキャンセルするため、結果としてＤＥＳ－ＳＳモードの部分のみが残るからである。

【０１３５】このとき、例えばブロックＢ３をブロックＢ１と同一の内容とすると、暗号化装置１０全体としては、ブロックＢ１とＢ２をそれぞれ拡大転置した出力を結合した１２８ビットの鍵を入力とするＤＥＳ－ＳＳと同一の処理内容となる。

【０１３６】上述したように、本発明の実施の形態に係る暗復号装置は、２５６ビットの鍵情報Ｋを５つのブロックに分割し、各ブロック情報を用いて実質的な中間鍵情報のみならず、第１，第２置換処理部１２，１４の使用有無、及び、第１，第２，第３暗復号化部１１，１３，１５の動作モード指定ができる情報を生成し、これによって装置全体の動作モードを制御するようにしたので、第１の実施形態と同様な装置を実現させ、その作用効果を得ることができる。

【０１３７】すなわち本実施形態では、鍵情報Ｋの内容を修正するだけで動作モードの変更を容易に行うことが

でき、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳのすべてと互換な単一の暗号アルゴリズムを構成するとともに、データの連続性に擾乱を起せる線形攻撃や差分攻撃等に強い暗号をも実現させることができる。

（発明の第３の実施の形態）本実施形態は、第２の実施形態における第１，第３暗復号化部１１，１５のＧ関数に改良を加えた場合について説明する。

【０１３８】図１１は本発明の第３の実施形態に係る暗復号装置におけるＧ関数の構成例を示すブロック図であり、図１～図１０と同一部分には同一符号を付して説明を省略する。

【０１３９】この暗復号装置１０は、図１１に示すように、第１，第３暗復号化部１１，１５のＧ関数８１ｇ～９６ｇにおいて、論理積１０１～排他的論理和１０３間に置換部１０２，論理積１０６～排他的論理和１０８間に置換部１０７が挿入される他、第２の実施形態と同様に構成されている。したがって、本実施形態にて説明するＧ関数８１ｇ～９６ｇは厳密にはＤＥＳ－ＳＳのＧ関数とは異なるものであり、ＤＥＳ－ＳＳ用のＧ関数が修正されたものである。

【０１４０】置換部１０２，１０７は、差分の一様性および非線形性の高い特性を有する，例えば図２に示すような置換表を保持しており、入力を置換表により変換して出力する。

【０１４１】このように構成された本実施形態の暗復号装置１０は第２の実施形態と同様に動作する他、新たな付加された置換部１０２，１０７部分については以下のように動作する。

【０１４２】まず、置換部１０２においては、論理積１０１の出力が入力されるようになっている。この論理積出力は置換表にて置換され、その結果が排他的論理和１０３に出力される。

【０１４３】また、置換部１０７においては、論理積１０６の出力が入力されるようになっている。この論理積出力は、置換部１０２の場合と同様に置換表にて置換され、その結果が排他的論理和１０８に出力される。

【０１４４】本実施形態のＧ関数８１ｇ～９６ｇでは、その中に差分確率及び線形確率が低い置換表による置換１０２，１０７が挿入されているために、データの連続性に擾乱が起こされ、線形攻撃や差分攻撃に強い暗号化が実現されている。

【０１４５】この置換部１０２，１０７に用いる置換表として、本実施形態では図２に示す表を用いると説明したが、この変形例として図２の置換表をアフィン変換して入力０に対する出力が０である置換表を用いることも考えられる。このとき、特定の鍵入力の場合には置換部１０２，１０７の出力が０となり、排他的論理和部１０３及び１０８における鍵情報の挿入が行われなくなる。したがって、このような置換表を用いた場合には、Ｇ関数は入力と出力が一致する恒等変換の関数として機能することも可能になる。

【０１４６】上記置換部１０２，１０７を用いることにより、論理積部１０１及び１０６における鍵との論理積の結果、論理積の出力ビットの０ビットと１ビットの出現率に不均一性が現れても、置換部１０２，１０７の処理により、この不均一性を是正し、鍵に含まれる１ビットの数に着目した攻撃に対して安全になる。

【０１４７】例えば拡大鍵Ｇ１に出現する１ビットの数が１個の場合には、排他的論理和部１０３においてささされる鍵、すなわち排他的論理和が行われる実質ビット数は高々１ビットである。しかし、置換部１０２による置換の結果、ささされる鍵のビット数は変化し、鍵に含まれる１ビットの数に着目した攻撃に対して安全になる。

【０１４８】上述したように、本発明の実施の形態に係る暗復号装置は、Ｇ関数に置換部１０２，１０７を挿入したので、データの連続性に擾乱が起こされ、線形攻撃や差分攻撃に強い暗号化を実現することができる。

【０１４９】なお、実施形態に説明した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【０１５０】ここで本発明における記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【０１５１】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【０１５２】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【０１５３】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【０１５４】なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【０１５５】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１５６】

【発明の効果】以上詳記したように本発明によれば、ＤＥＳ、トリプルＤＥＳ、ＤＥＳ－ＳＳのすべてと互換な単一の暗号アルゴリズムを構成するが、単にＤＥＳ－ＳＳを３段重ねるより効率がよく、かつ差分攻撃や線形攻撃にも強いアルゴリズムとなる暗復号装置及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る暗復号装置の一例を示す構成図。

【図２】置換処理部等に用いられる差分確率及び線形確率の低い置換表の一例を示す図。

【図３】各機能部の状態組み合わせの例を示す図。

【図４】鍵スケジュール部の全体構成を示す図。

【図５】拡大転置表の一例を示す図。

【図６】ＤＥＳ－ＳＳ鍵スケジュール部の構成例を示すブロック図。

【図７】置換用鍵スケジュール部の構成例を示すブロック図。

【図８】置換処理部の構成例を示すブロック図。

【図９】ＤＥＳ－ＳＳとして構成された暗復号化部の構成例を示すブロック図。

【図１０】Ｇ関数の構成例を示すブロック図。

【図１１】本発明の第３の実施形態に係る暗復号装置におけるＧ関数の構成例を示すブロック図。

【符号の説明】

１０…暗復号装置
１１…第１暗復号化部
１２…第１置換処理部
１３…第２暗復号化部
１４…第２置換処理部
１５…第３暗復号化部
１６…鍵スケジュール部
２１…平文
２２…暗号文
＊３１…分割部
３７…拡大転置部
３８，３９…ＤＥＳ－ＳＳ鍵スケジュール部
４０…ＤＥＳ鍵スケジュール部
４１…置換用鍵スケジュール部
４５…Ａスケジュール部
４６…Ｂスケジュール部
４７…ＦＧ拡大鍵生成部
４８Ａ，４８Ｂ…ビット選択部
４９，５０…排他的論理和
５５，５８…論理和部
５６…左シフト部
６１…初期転置部
６２～６６…排他的論理和
６７～７４…置換部
７５…逆転置部
８０…初期転置部
８１～９６…データ攪拌部
８１ａ～９６ａ…排他的論理和
８１ｆ～９６ｆ…Ｆ関数
８１ｇ～９６ｇ…Ｇ関数
９７…最終転置部
１０１，１０６…論理積部
１０２，１０７…置換部
１０３，１０４，１０８…排他的論理和部
１０５…左シフト部
Ｂ１～Ｂ４…ブロック
ＦＫ…Ｆ関数拡大鍵
Ｇ１～Ｇ４…拡大鍵
ＧＫ…Ｇ関数拡大鍵
Ｋ１…第１暗復号化部への中間鍵
Ｋ２…第２暗復号化部への中間鍵
Ｋ３…第３暗復号化部への中間鍵
ＫＫ１…第１置換処理部への中間鍵
＊　ＫＫ２…第２置換処理部への中間鍵

【図２】

置換表

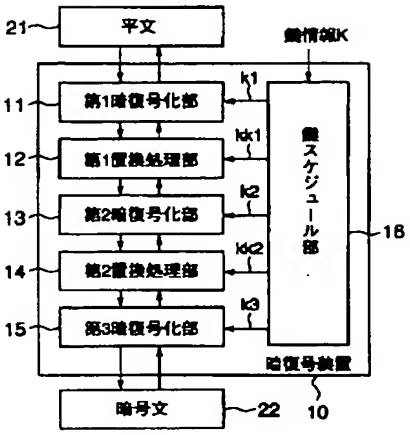
0	1	142	244	71	187	122	186	173	157	221	152	61	170	93	150
216	114	192	88	224	62	76	102	144	222	85	128	160	131	75	42
108	247	57	81	96	86	44	138	112	208	31	74	38	139	51	110
72	137	111	46	164	195	64	94	80	34	207	169	171	12	21	225
54	95	248	213	146	78	166	4	48	136	43	30	22	103	69	147
56	35	194	140	129	29	37	97	19	193	203	99	151	14	55	65
36	87	202	91	185	196	23	77	82	141	239	179	32	236	47	50
40	209	17	217	235	167	203	121	219	119	6	187	132	205	254	252
27	84	161	29	124	204	228	176	73	49	39	45	83	105	2	245
24	223	68	79	155	188	15	92	11	220	189	148	172	9	199	162
28	130	159	198	52	194	70	5	206	63	13	60	156	8	190	183
135	229	238	107	233	242	191	175	197	100	7	123	149	154	174	182
18	89	165	53	101	184	163	158	210	247	98	90	133	125	168	58
41	113	200	246	249	67	215	214	16	115	118	120	153	10	26	145
20	61	230	240	134	177	226	241	250	116	243	180	109	33	178	106
227	231	181	234	3	143	211	201	66	212	232	117	127	255	126	253

【図５】

拡大転置表

1	2	3	4	5	6	7	8	0	9	10	11	12	13	14	15
16	0	17	18	19	0	20	21	0	22	23	24	25	26	27	28
29	30	0	31	32	0	33	34	35	36	0	37	38	39	40	41
42	43	44	45	46	0	47	48	49	50	51	52	53	54	55	56

【図１】

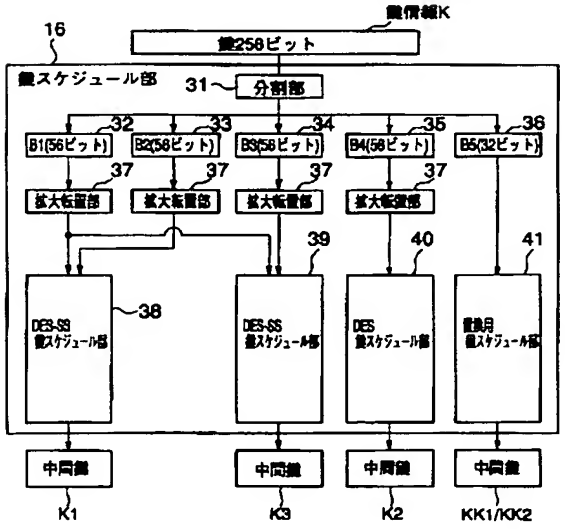


【図３】

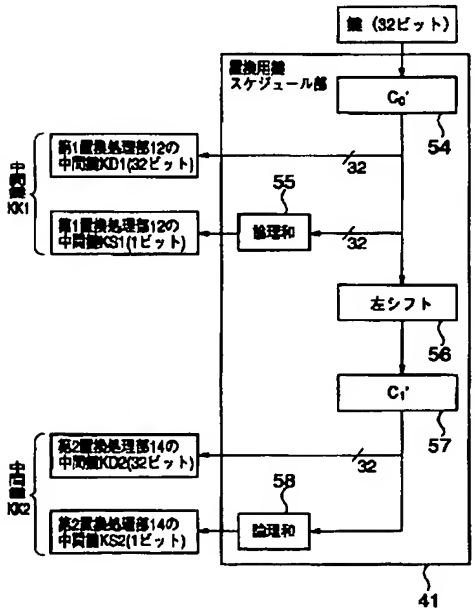
	互換モード			強化暗号モード		
第1暗復号化部	DES	DES	DES	DES-SS	DES	
第1置換処理部	未使用	未使用	未使用	使用	使用	
第2暗復号化部	DES	DES	DES	DES	DES	・・・
第2置換処理部	未使用	未使用	未使用	使用	使用	
第3暗復号化部	DES	DES	DES-SS	DES-SS	DES	
得られる暗号	DES *1	トリプルDES *2	DES-SS *3	パターン1	パターン2	・・・

*1：第1、第2暗復号化部で同一の鍵を使用する
*2：第1、第3暗復号化部で同一の鍵、第2暗復号化部で異なる鍵を使用する
*3：第1、第2暗復号化部で同一の鍵を使用する

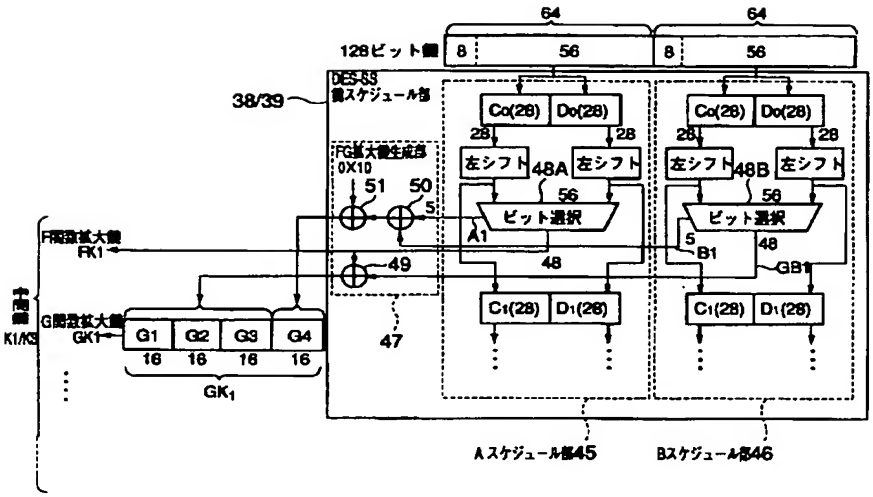
【図４】



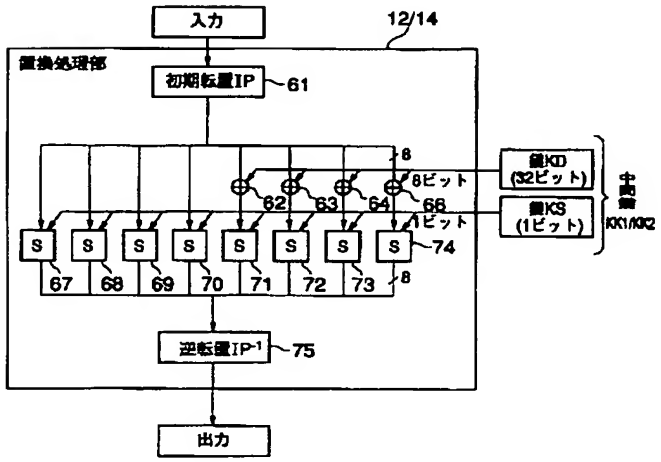
【図７】



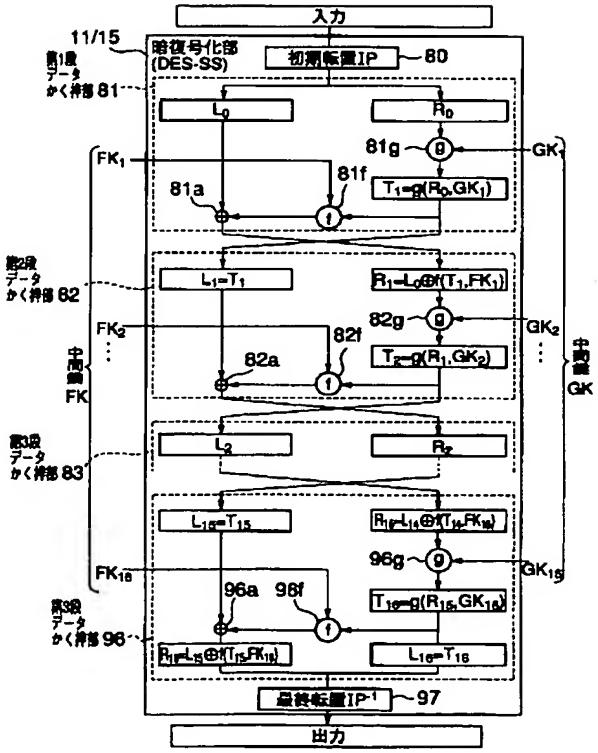
【図６】


64
64
128ビット鍵
8
56
8
56
DES-SS
鍵スケジュール部
38/39
Co(28)
Do(28)
28
28
左シフト
48A
左シフト
FG拡大鍵生成部
0X10
51
50
5
56
ビット選択
A1
48
49
C1(28)
D1(28)
47
左シフト
48B
左シフト
B1
GB1
F関数拡大鍵
FK1
中間鍵
K1/K2
G関数拡大鍵
GK1
G1
G2
G3
G4
16
16
16
16
GK1
Aスケジュール部45
Bスケジュール部46

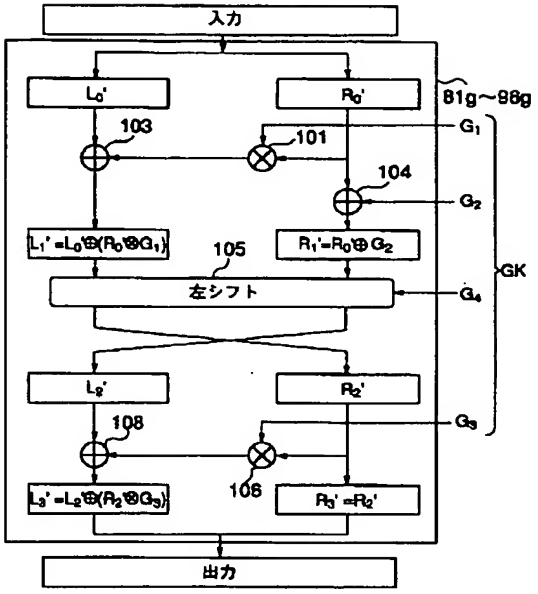
【図８】


入力
12/14
置換処理部
初期転置IP
61
8
8ビット
62
63
64
66
1ビット
鍵KD
(32ビット)
鍵KS
(1ビット)
中間鍵
KK1/KK2
S
S
S
S
S
S
S
S
74
67
68
69
70
71
72
73
8
逆転置IP-1
75
出力

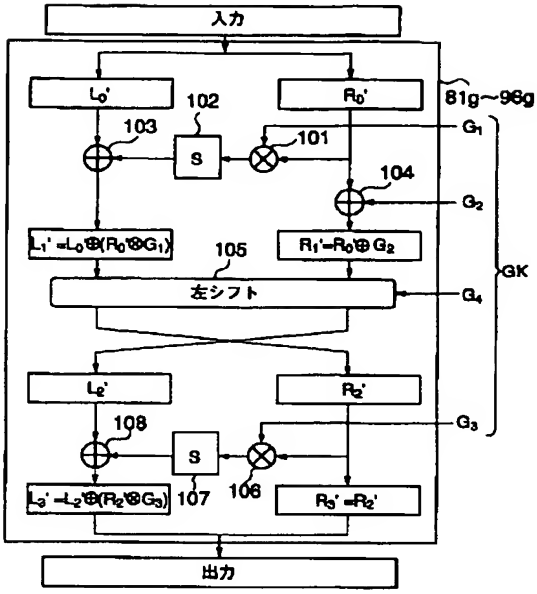
【図９】


入力
11/15
暗復号化部
(DES-SS)
初期転置IP
80
第1段
データ
かく拌部81
L0
R0
81g
GK1
FK1
81f
81a
T1=g(R0,GK1)
第2段
データ
かく拌部82
L1=T1
R1=L0⊕f(T1,FK1)
82g
GK2
FK2
82f
82a
中間鍵
FK
中間鍵
GK
第3段
データ
かく拌部83
L2
R2
L15=T15
R16=L14⊕f(T15,FK16)
96g
GK16
FK16
96a
96f
T16=g(R15,GK16)
第3段
データ
かく拌部96
R16=L15⊕f(T15,FK16)
L16=T16
最終転置IP-1
97
出力

【図１０】



【図１１】



フロントページの続き

(72)発明者　清水　秀夫
東京都府中市東芝町１番地　株式会社東芝
府中工場内

Ｆターム(参考)　5J104 AA18 AA41 JA15 NA02 NA09
NA27 PA07